

(19) 日本国特許庁 (JP)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-30171

(P2000-30171A)

(43) 公開日 平成12年1月28日(2000.1.28)

(51) Int.Cl.<sup>7</sup>  
 G 0 8 B 25/04  
 // G 0 6 F 17/60

識別記号

F I  
 G 0 8 B 25/04  
 G 0 6 F 15/21

テマコード\*(参考)  
 A 5 B 0 4 9  
 L 5 C 0 8 7

審査請求 未請求 著求項の数4 O.L. (全5頁)

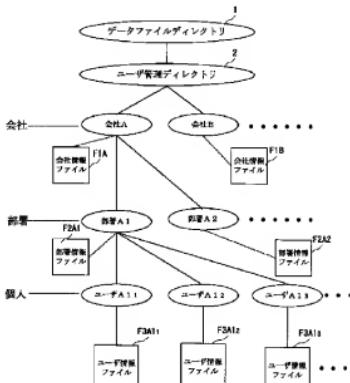
(21) 出願番号	特願平10-200265	(71) 出願人	000006666 株式会社山武 東京都渋谷区渋谷2丁目12番19号
(22) 出願日	平成10年7月15日(1998.7.15)	(72) 発明者	早川 繁 東京都渋谷区渋谷2丁目12番19号 株式会 社山武内
		(74) 代理人	100064621 弁理士 山川 政樹
			Fターム(参考) 5B049 CC21 CC45 DD05 ED05 FF07 FF09 5C087 CC52 DD03 DD23 ED07 FF19 FF20 GG07 GG18 GG19 GG21 GG24 GG32 GG51 GG66

## (54) 【発明の名称】 アクセス権レベル設定方法

## (57) 【要約】

【課題】 ビル管理者の作業負担を大幅に軽減する。会社側のプライバシーを守る。

【解決手段】 ビル内のユーザを「会社」、「部署」、「個人」の階層構造として分類し、ビル管理者に「会社」のアクセス権レベル（会社の責任者のアクセス権とその会社がアクセスできる機能および機器）を設定させ、「会社」の責任者に「部署」のアクセス権レベル（部署の責任者のアクセス権とその部署がアクセスできる機能および機器）を設定させ、「個人」のアクセス権レベル（ユーザのアクセス権とそのユーザがアクセスできる機能および機器）を設定させること。



## 【特許請求の範囲】

【請求項1】 ビル内のユーザー毎にビル管理システムの情報へのアクセス権レベルを設定するアクセス権レベル設定方法において、

前記ビル内のユーザーをその所属により第1～第nの階層構造として分類し、ビル管理者に第1階層のアクセス権レベルを設定させ、第1階層の責任者に第2階層のアクセス権レベルを設定させるというようにして各階層のアクセス権レベルを設定させ、第n-1の階層の責任者に第nの階層である「個人」のアクセス権レベルを設定させることを特徴とするアクセス権レベル設定方法。

【請求項2】 ビル内のユーザー毎にビル管理システムの情報へのアクセス権レベルを設定するアクセス権レベル設定方法において、

前記ビル内のユーザーを「会社」、「部署」、「個人」の階層構造として分類し、ビル管理者に「会社」のアクセス権レベルを設定させ、「会社」の責任者に「部署」のアクセス権レベルを設定させ、「部署」の責任者に「個人」のアクセス権レベルを設定させるようにすることを特徴とするアクセス権レベル設定方法。

【請求項3】 ビル内のユーザー毎にビル管理システムの情報へのアクセス権レベルを設定するアクセス権レベル設定方法において、

前記ビル内のユーザーをその所属により第1～第nの階層構造に分類した各階層の管理情報を記憶するメモリと、このメモリに記憶された各階層の管理情報に対してアクセス権レベルを付加するアクセス権レベル付加手段とを備え、

前記アクセス権レベル付加手段において、第1階層の管理情報に対するアクセス権レベルはビル管理者によって付加され、第2階層以上のアクセス権レベルは直上の階層の責任者によって付加されることを特徴とするアクセス権レベル設定方法。

【請求項4】 ビル内のユーザー毎にビル管理システムの情報へのアクセス権レベルを設定するアクセス権レベル設定方法において、

前記ビル内のユーザーをその所属により「会社」、「部署」、「個人」の階層構造に分類した各階層の管理情報を記憶するメモリと、

このメモリに記憶された各階層の管理情報に対してアクセス権レベルを付加するアクセス権レベル付加手段とを備え、

前記アクセス権レベル付加手段において、「会社」の管理情報に対するアクセス権レベルはビル管理者によって付加され、「部署」の管理情報に対するアクセス権レベルは「会社」の責任者によって付加され、「個人」の管理情報に対するアクセス権レベルは「部署」の責任者によって付加されることを特徴とするアクセス権レベル設定方法。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】この発明は、ビル内のユーザー毎にビル管理システムの情報へのアクセス権レベルを設定するアクセス権レベル設定方法に関するものである。

## 【0002】

【従来の技術】通常、ビルには複数の会社が入居しており、これらの会社に勤務する人達（ユーザー）には各自にビル管理システムの情報へのアクセス権が与えられている。

10) このアクセス権は、そのレベル（アクセス権レベル）が段階的に分かれており、アクセス権レベルの高い人はほど重要な情報にアクセスすることができる。従来より、このユーザーに対するアクセス権レベルの設定は、ビル管理者側で行っている。

【0003】なお、ビル管理システムは、ビル内の各種管理ポイントの状態や各種管理ポイントへの発停等の情報を管理するシステムであり、ビル内の中央監視室などに配置され、ビル管理者にその運用が任される。

【0004】図6に従来のアクセス権レベルの設定例20)（ユーザ情報例）を示す。ビル管理者は、ビル内の全てのユーザー（社員）に対し、ビル管理システムの情報へのアクセス権レベルを設定する。アクセス権レベルは、運転員、運転管理者、施設管理者、システム管理者の4段階となっており、例えば、運転員は表示のみを参照することができ、運転管理者は設備に対する設定や変更まで行うことができ、施設管理者はデータ管理まで行うことができ、システム管理者は全体のシステム管理まで行うことができる。

## 【0005】

30) 【発明が解決しようとする課題】しかしながら、このような従来のアクセス権レベルの設定方法によると、ユーザーに対するアクセス権レベルの設定がビル管理者1人に任せられていたため各種の問題が生じていた。例えば、会社へ人員移動があり、アクセス権レベルを変更する必要が生じたとする。この場合、会社Aの責任者は、異動者のアクセス権レベルをビル管理者に伝える。これを受けて、ビル管理者は、図6に示したようなユーザ情報において、異動者のアクセス権レベルを変更する。ところが、ビル内のユーザーはそれぞれ独自にレイアウトを変更したり、また会社の入退去が、不定期に発生する。また、部署間の人の異動者も不定期で起こり得る。このため、ビル管理者は、ユーザーと会社の責任者との連絡を密にする必要がある。また、これら不定期に発生する事態において、ビル管理者がユーザー個人までアクセス権レベルの設定（新規登録も含む）／変更を行う必要があり、膨大な作業量が発生する。一方、会社側では、部署や個人に関する情報までビル管理者に連絡しなければならず、プライバシーの問題等からなるべく公にしたくはないという亂潮が生じている。

40) 【0006】本発明はこのような課題を解決するために

なされたもので、その目的とするところは、ビル管理者の作業負担を大幅に軽減することができ、また会社間のプライバシーを守ることもできるアクセス権レベル設定方法を提供することにある。

#### 【0007】

【課題を解決するための手段】このような目的を達成するために、本発明は、ビル内のユーザをその所属により第1～第nの階層構造として分類し、ビル管理者に第1階層（例えば、「会社」）のアクセス権レベルを設定させ、第1階層の責任者に第2階層（例えば、「部署」）のアクセス権レベルを設定させるというようにして各階層のアクセス権レベルを設定させ、第n-1の階層（例えば、「部署」）の責任者に第nの階層である個人のアクセス権レベルを設定させるようにしたものである。この発明によれば、例えば、ビル管理者が「会社」のアクセス権レベルを設定し、会社の責任者が「部署」のアクセス権レベルを設定し、「部署」の責任者が「個人」のアクセス権レベルを設定する。

#### 【0008】

【発明の実施の形態】以下、本発明を実施の形態に基づき詳細に説明する。図1はこの発明を適用して構築された会社・部署・ユーザ管理データ構造を示す図である。このデータ構造では、データファイルディレクトリ1の下にユーザ管理ディレクトリ2が置かれ、ユーザ管理ディレクトリ2の下に会社・部署・ユーザ管理データ構造が構築されている。

【0009】この会社・部署・ユーザ管理データ構造では、ビル内のユーザを「会社」、「部署」、「個人」の階層構造として分類し、ビル管理者に「会社」のアクセス権レベル（会社の責任者のアクセス権とその会社がアクセスできる機能および機器）を設定させ、「会社」の責任者に「部署」のアクセス権レベル（部署の責任者のアクセス権とその部署がアクセスできる機能および機器）を設定させ、「部署」の責任者に「個人」のアクセス権レベル（ユーザのアクセス権とそのユーザがアクセスできる機能および機器）を設定させている。

【0010】ユーザ管理ディレクトリ2には、会社A、会社B・・・のディレクトリの下に、会社A、B・・・の情報ファイル（会社情報ファイル）F1 A、F1 B・・・が作成されている。会社Aに属する部署A1、A2・・・のディレクトリの下に、部署A1、A2・・・の情報ファイル（部署情報ファイル）F2 A1、F2 A2・・・が作成されている。部署A1に属するユーザA1、A1z、A1s・・・のディレクトリの下に、ユーザA1、A1z、A1s・・・の情報ファイル（ユーザ情報ファイル）F3 A1 1、F3 A1 2、F3 A1 3・・・が作成されている。会社B・・・についても同様にして会社情報ファイル、部署情報ファイル、ユーザ情報ファイルが作成されている。

【0011】図2に会社情報ファイルF1、図3に部署

情報ファイルF2、図4にユーザ情報ファイルF3の具体例を示す。これらのファイルF1、F2、F3はRAM5（図5参照）中に記憶される。図5において、3はCPU、4はROM、5はRAM、6、7はインターフェイスである。CPU1は、インターフェイス6、7を介して与えられるシステムからの各種入力情報を得て、ROM4に格納されたプログラムに従い、RAM5にアクセスしながら、各種処理動作を行う。

#### 【0012】

【0012】会社情報ファイルF1には、会社の管理情報が記入されている。まず、会社名、管理者（会社の責任者）名、管理者電話番号、管理者FAX番号、管理者のメールアドレス、メモ情報等が登録されている。また、会社属性として、ビル管理会社であるか、メンテナンスを行う会社であるか、ある施設または設備の管理会社であるかの情報が記入されている。この会社情報ファイルF1はビル管理者が作成する。この作成された会社情報ファイルF1をCPU3がRAM5中に記憶させる。

#### 【0013】

部署情報ファイルF2には、部署の管理情報が記入されている。まず、部署名、部署管理者（部署の責任者）名、部署管理者電話番号、部署管理者FAX番号、部署管理者メールアドレス、メモ情報等が登録されている。また、部署属性として、ビル管理部署であるかどうか、メンテナンスを行う部署であるかどうか、ある施設または設備の管理部署であるかどうかの情報が記入されている。この部署情報ファイルF2は会社の責任者が作成する。この作成された部署情報ファイルF2をCPU3がRAM5中に記憶させる。

#### 【0014】

ユーザ情報ファイルF3には、ユーザのログイン名、パスワード、名前、電話番号、FAX番号、メールアドレス、メモ情報等が登録されている。また、ユーザ属性として、このユーザがビル管理者であるかどうか、メンテナンスを行う人かどうか、ある施設または設備の管理者かどうか、会社管理者かどうか、部署管理者かどうか、一般ユーザかどうかの情報が記入されている。このユーザ情報ファイルF3は部署の責任者が作成する。この作成されたユーザ情報ファイルF3をCPU3がRAM5中に記憶させる。

#### 【0015】

ビルに新規に会社が入居した場合、ビル管理者が該当する会社の会社情報ファイルF1を登録する。また、会社の責任者が変わった場合、ビル管理者が該当する会社の会社情報ファイルF1の内容を変更する。また、ビルから会社が移転した場合、ビル管理者が該当する会社の会社情報ファイルF2を削除する。会社の責任者は、部署の変更等に応じて、部署情報ファイルF2を変更／削除する。部署の責任者は、ユーザの異動等に応じて、ユーザ情報ファイルF3を変更／削除する。

【0016】このように、本実施の形態によるアクセス権レベル設定方法によれば、ビル管理者は会社情報ファ

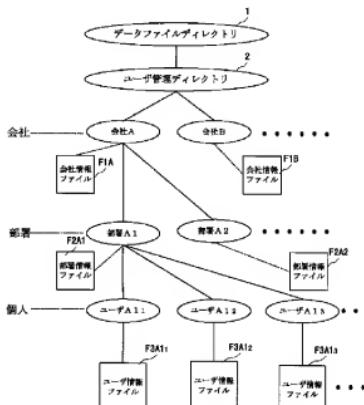
イルF1を登録したり、変更したり、削除したりするのみでよいので、ビル管理者の作業負担が大幅に軽減される。また、本実施の形態によるアクセス権レベル設定方法によれば、会社の責任者や部署の責任者は部署情報ファイルF2やユーザ情報ファイルF3を登録したり、変更したり、削除したりするのみでよく、会社側から部署や個人に関する情報をビル管理者に連絡しなくてもよいので、プライバシーを守ることができるようになる。

【0017】なお、上述した実施の形態では、ビル内のユーザを「会社」、「部署」、「個人」の階層構造として分類したが、階層構造は「会社」、「部署」、「個人」に限ることではなく、種々の階層構造が考えられる。

(0018)

【発明の効果】以上説明したことから明らかなように本発明によれば、例えば、ビル管理者に「会社」のアクセス権レベルを設定させ、会社の責任者に「部署」のアクセス権レベルを設定させ、「部署」の責任者に「個人」のアクセス権レベルを設定させるようすることにより、ビル管理者の作業負担を大幅に軽減することができ、また会社側のプライバシーを守ることもできるようになります。

【図1】



176

#### 【図面の簡単な説明】

【図1】 本発明を適用して構築された会社・部署・ユーザ管理データ構造を示す図である

【図2】 会社情報ファイルの具体例を示す図である。

【図3】 部署情報ファイルの具体例を示す図である

【図4】 ユーザ情報ファイルの具体例を示す図である

【図5】この発明が適用された装置の要部構成を示す  
ブロック図である

【図6】 従来のアクセス権レベルの設定例（ユーザ情報図）を示す図である。

#### 【符号の説明】

1…データファイルディレクトリ、2…ユーザ管理ディレクトリ、F1(F1A, F1B, …)…会社情報ファイル、F2(F2A1, F2A2, …)…部署情報ファイル、F3(F3A1, F3A2, …)…F3A1, …)…ユーザ情報ファイル、3…CPU、4…ROM、5…RAM、6…7…インターフェイス

[圖2]

【図3】

絶縁接続ファイル

```

転送用データを入力するための接続情報を記載されている。
<SECTION_NAME>
<ADMINISTRATOR_NAME>
  ユーザーの管理者名を入力。
<ADMINISTRATOR_PASSWORD>
  パスワードを入力する。
<ADMINISTRATOR_TYPE>
  ユーザーの権限を入力する。
<ADMINISTRATOR_EMAIL>
  管理者用のEメールアドレスを入力する。
<ADMINISTRATOR_PHONE>
  フォン番号を入力。
<ADMINISTRATOR_FAX>
  フax番号のFAX番号を入力する。
<ADMINISTRATOR_PAGER>
  ページャー番号を入力。
<ADMINISTRATOR_NILLL>
  デフォルト: NILLL
  メール送信用のメールアドレスを入力する。
<DEFINITE_MAIL>
  デフォルト: NILLL
  メール送信用のメールアドレスを入力する。
<DEFINITE_FAX>
  デフォルト: NILLL
  フax送信用のFAX番号を入力する。
<DEFINITE_PAGER>
  デフォルト: NILLL
  ページャー番号を入力する。
<DEFINITE_PHONE>
  デフォルト: NILLL
  フォン番号を入力する。
<DEFINITE_FAX>
  デフォルト: NILLL
  フax番号を入力する。
  この例では、ユーザーのメールアドレスのところにディフォルトとして表示されるNilLl表示。
<DEFAULT_MAIL>
  デフォルト: NILLL
  メール送信用のメールアドレスを入力する。
  この例では、メール送信用のメールアドレスを入力するとき、その実際の、ユーザーのメールアドレスのところにディフォルトとして表示されるNilLl表示。
<DEFINITE_PHONE>
  デフォルト: NilLl
  フォン番号を入力する。
  この例では、ユーザーの電話番号のところにディフォルトとして表示されるNilLl表示。
<DEFINITE_PAGER>
  デフォルト: NilLl
  ページャー番号を入力する。
  この例では、ユーザーのページャー番号のところにディフォルトとして表示されるNilLl表示。
<DEFINITE_FAX>
  デフォルト: NilLl
  フax番号を入力する。
  この例では、ユーザーのfax番号のところにディフォルトとして表示されるNilLl表示。
<DEFINITE_ADMIN>
  デフォルト: Admin
  ユーザーの管理者名を入力する。
  この例では、ユーザーの管理者名のところにディフォルトとして表示されるAdmin表示。
<ADMIN_PASSWORD>
  パスワードを入力する。
  この例では、ユーザーのパスワードのところにディフォルトとして表示されるAdmin表示。

```

【図4】

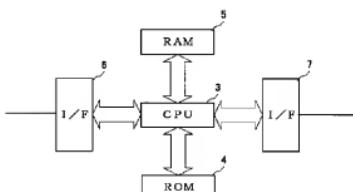
ユーザー登録ファイル

```

ユーザー登録ファイルは複数あると、ユーザーの登録情報を記入されている。
ユーザー登録ファイルには、以下の項目が記入する。
<LINK_NAME>
  リンク名を入力。
<PARENT>
  ルートの親リンク名を入力する。
<NAME>
  ユーザーの名前を入力する。
<EMAIL>
  ユーザーのEメールを記入する。
<PHONE>
  ユーザーの電話番号を記入する。
<FAX>
  ユーザーのFAX番号を記入する。
<PAGER>
  ユーザーのページャー番号を記入する。
<DEFINITE>
  ユーザーのメールアドレスを記入する。
<DEFINITE_PHONE>
  ユーザーの電話番号を記入する。
<DEFINITE_FAX>
  ユーザーのfax番号を記入する。
<DEFINITE_PAGER>
  ユーザーのページャー番号を記入する。
また、ユーザー登録上に以下アカウントが存在し、該当するならばTrue、該当しないならばFalseを記入する。
<ISADMIN>
  ユーザーが管理者である。
<ISOPERATOR>
  ユーザーが操作員である。
<ISMANAGER>
  ユーザーが管理者である。
<ISMEMBER>
  ユーザーが会員である。
<ISDEFINITE>
  ユーザーが登録された時刻(たとえば、セキュリティシステムや監視システム)の登録度である。
<ISDEFINITE_ADMIN>
  ユーザーが管理者である。
<ISDEFINITE_OPERATOR>
  ユーザーが操作員である。
<ISDEFINITE_MANAGER>
  ユーザーが管理者である。
<ISDEFINITE_MEMBER>
  このユーザーはこのユーザーが属する会員の会員登録である。
<ISDEFINITE_USER>
  ユーザーが会員である。
<ISDEFINITE_ANONYMOUS>
  このユーザーはこのユーザーが属する会員の匿名登録である。

```

【図5】



【図6】

社員番号	社員名	パスワード	レベル
0023	オヤマ	xxxxx	BBCCC
1035	イイジマ	xxxxx	AAAAA
0042	イケダ	xxxxx	CCBBC
1153	ウチダ	xxxxx	ABAAA
0054	オオタ	xxxxx	CCCB
0063	カネマル	xxxxx	DDDDD
*	*	*	*
*	*	*	*
*	*	*	*
*	*	*	*
*	*	*	*
*	*	*	*
*	*	*	*
*	*	*	*